The opportunities and limits of data portability for stimulating competition and innovation

Graef, Inge

Published in:
Competition Policy International - Antitrust Chronicle

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

THE OPPORTUNITIES AND LIMITS OF DATA PORTABILITY FOR STIMULATING COMPETITION AND INNOVATION

BY INGE GRAEF[1]

1 Associate Professor of Competition Law at Tilburg University, affiliated to the Tilburg Law & Economics Center (TILEC) and the Tilburg Institute for Law, Technology, and Society (TILT). This article is based on oral remarks made by the author at the 'Data To Go' workshop on data portability organized by the US Federal Trade Commission on September 22, 2020. For more information about the workshop, see https://www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.

CPI ANTITRUST CHRONICLE
NOVEMBER 2020

CPI Talks…
…with Jon Leibowitz

Data to Go: The Ftc's Workshop on Data Portability
By Guilherme Roschke & Andrea Zach

Data Portability
By Daniel L. Rubinfeld

Using the Portability and Other Required Transfers Impact Assessment ("Port-Ia") in Antitrust Law
By Peter Swire & John Snyder

Unpacking Data Portability
By Christopher S. Yoo

The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation
By Inge Graef

Online Search Competition and the Risk of Unintended Consequences of Data Access
By Jordi Casanova

The Impact of Data Portability on Platform Competition
By Emanuele Giovannetti & Paolo Siciliani

Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data
By Daniel Gill & Wolfgang Kerber

Data Access and Portability and EU Competition Law
By Björn Lundqvist

CPI Antitrust Chronicle November 2020

www.competitionpolicyinternational.com

I. INTRODUCTION

The concept of data portability has been heralded as a key enabler of consumer empowerment, competition and innovation. Despite its potential, data portability does not seem to have had the impact yet it was expected to have. Against this background, this article explores the opportunities as well as limits of data portability and provides suggestions to make data portability more effective – both as a data protection concept and as a tool for stimulating competition and innovation.

To reap its full potential, this article submits that there is a need for regulators to steer the implementation of the right to data portability in the General Data Protection Regulation ("GDPR") through guidance to data controllers on how to balance different interests and through asymmetric enforcement by imposing additional requirements on data controllers with market power. Attention is also paid to merger review, where the GDPR's right to data portability has been relied upon as a limit that can prevent competition concerns from arising despite the current problems with data protection enforcement. Because of its hybrid nature that brings together considerations of data protection, competition and innovation, data portability can also be implemented through other regimes beyond data protection law. In particular, data portability may be imposed under competition law on dominant firms and under the upcoming ex ante regulation in the Digital Markets Act on gatekeeping platforms. These regimes are not bound by the limits of the GDPR's right to data portability and can therefore impose additional forms of data portability, including portability of non-personal data for business users, portability of inferred data and real-time continuous portability. The article concludes that, nevertheless, data portability in itself is unlikely to be sufficient in order to address the risk of market tipping and to keep data-driven markets open to newcomers.

II. HYBRID NATURE OF DATA PORTABILITY

The nature of data portability is a hybrid between various interests. The concept originated in the GDPR, which is a data protection instrument and aims to empower individuals by strengthening the control over their personal data. The right to data portability of Article 20 GDPR was one of the tools introduced to pursue this objective by giving individuals the right to receive personal data provided to a data controller in a structured, commonly used and machine-readable format and to transmit this data to another controller. In this sense, one can argue that the right to data portability fits with the fundamental rights nature of data protection by enhancing informational self-determination.[2]

2 Orla Lynskey, "Aligning data protection rights with competition law remedies? The GDPR right to data portability," European Law Review 2017, p. 809-810.

At the same time, one can characterize data portability by the sharing and reuse of data that it facilitates.[3] During the legislative discussions in the Council, a number of Member States doubted whether to retain the right to data portability in the GDPR because they considered data portability not to be within the scope of data protection but rather in consumer or competition law.[4] However, one should keep in mind that the GDPR serves a dual objective of, on the one hand, protecting the fundamental right to data protection and, on the other hand, promoting the free flow of personal data.[5] This second objective, which is more about stimulating the EU's internal market, is very much present in the right to data portability and brings the concept close to other policy areas, in particular those of competition and innovation.

In EU law and policymaking, the concept of data portability is now emerging in many areas: from data protection to consumer law,[6] it has been integrated into competition analysis already in some merger cases,[7] and it also forms part of broader innovation policies for instance in the context of the European Commission's data strategy.[8] In addition, notions of data portability and data access are appearing in sector-specific frameworks, for instance in the banking,[9] energy[10] and automotive[11] industries. This makes data portability a concept with a hybrid nature. This hybrid nature also determines what impact data portability can have on consumers and competition. Because of the various interests that come together in the concept of data portability, there are still questions about how tensions between these interests should be reconciled in concrete cases. These tensions can stand in the way of data portability reaching its potential for stimulating data protection, competition and innovation.

III. OVERLAPPING LEGAL ENTITLEMENTS

The existence of different legal entitlements over the same dataset can result into tensions between the various interests relevant to data portability. This issue takes different shapes. Personal data can relate to more than one individual, for instance one's interactions on a social network. And personal data of an individual may at the same time be protected by intellectual property rights held by a data controller.

Such overlapping legal entitlements can limit the effectiveness of data portability, depending on the extent to which they stand in the way of requests of individuals to have their personal data transferred to another provider. For example, Facebook has claimed before that its trade secrets and intellectual property prevent the company from sharing all the personal data it holds about a user in response to access requests under data protection law.[12] How exactly these interests and legal entitlements should be balanced against each other is not entirely clear from the text of the GDPR.

Article 20(4) GDPR states that the application of the right to data portability should not adversely affect the rights and freedoms of others. Such third-party rights and freedoms include the data protection rights of others as well as the intellectual property rights held by data controllers. Some guidance on how to balance these interests has been provided by the Article 29 Working Party[13] in its 2017 guidelines on the right to data portability.

---

3 Inge Graef, Martin Husovec & Nadezhda Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law," German Law Journal 2018, p. 1369.

4 Council of the European Union, Interinstitutional File: 2012/0011 (COD), 10614/14, June 6, 2014, p. 3 footnote 1.

5 Article 1 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) [2016] OJ 119/1.

6 Article 16(4) of Directive (EU) 2019/770 of the European Parliament and of the Council of May 20, 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Digital Content Directive) [2019] OJ L 136/1.

7 See Case M.7813 - Sanofi/Google/DMI JV, February 23, 2016 and Case M.8124 - Microsoft/LinkedIn, 6 December 2016 as discussed in section VI. below.

8 Commission Communication, "A European strategy for data," COM(2020) 66 final, 19 February 2020, p. 20.

9 Article 66 and 67 of Directive (EU) 2015/2366 of November 25, 2015 on payment services in the internal market (Payment Services Directive 2) [2015] OJ L 337/35.

10 Article 23 of Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity (Electricity Directive) [2019] OJ L 158/125.

11 See the discussion in Commission Communication, "On the road to automated mobility: An EU strategy for mobility of the future," COM (2018) 283 final, May 17, 2018, p. 13

12 Emil Protalinski, "Facebook: Releasing your personal data reveals our trade secrets," ZDNet, October 12, 2011, available at https://www.zdnet.com/article/facebook-releasing-your-personal-data-reveals-our-trade-secrets/.

13 The Article 29 Working Party is a former advisory body composed of, among others, representatives from the national data protection authorities in the EU Member States and is now replaced by the European Data Protection Board.

As regards mixed datasets containing personal data from more than one individual, the guidelines from the Article 29 Working Party suggest data controllers to set up mechanisms to obtain consent from third parties. This would ease data transmission in situations where third party data subjects are willing to consent to the porting of their personal data in response to someone else's data portability request. In the absence of such consent, the new data controller should identify another legal basis for the processing of third party personal data, such as its legitimate interests to provide a service to the data subject that invoked the data portability request. Beyond this purpose, the data controller is not allowed to use the transmitted third party data to serve its own interests, for instance for proposing marketing products or for enriching the profile of the third party data subject.[14]

With regard to intellectual property rights, the Article 29 Working Party states in its guidelines that intellectual property cannot be a reason for data controllers to refuse to port all the personal data. Data controllers should try to transmit personal data in a form that does not release information covered by trade secrets or intellectual property rights.[15] However, the guidelines do not clarify what should happen in case this is not possible. And if data controllers would be obliged to facilitate portability requests for personal data over which they hold intellectual property claims, another question is whether this also implies that new controllers should be able to reuse the ported data free of charge without having to obtain a license from the original intellectual property rights holder.[16] More clarity about these issues will hopefully follow, now the European Commission announced in its February 2020 Communication 'A European strategy for data' its intention to evaluate the intellectual property framework with a view to further enhance data access and use, including a possible clarification of the application of the Trade Secrets Directive as an enabling framework.[17]

How to precisely strike the balance between different interests will need to be addressed through future measures and cases. Despite the (non-legally binding) guidance from the Article 29 Working Party, the concrete application of the right to data portability in practice still raises issues. This can also be seen from the White Paper on data portability that Facebook published in September 2019 to launch a debate about how to develop privacy-protective data portability.[18] In addition, Facebook called upon regulators to step in to balance the desirability of data portability with the greater risks for privacy when announcing a photo transfer tool.[19] These are important trade-offs that should not be completely left up to private companies.[20]

Until more clarity is provided through further guidance or cases, there is quite some discretion for data controllers themselves to strike the balance between the various interests. This may not always lead to desirable outcomes, because data controllers could point to the existence of these overlapping legal entitlements as an excuse to limit the scope of the data that should be ported.

The message here is that the impact of data portability is not an abstract or static issue; it is something that regulators and enforcers can and should influence by guiding and steering implementation. This is true for how data portability interacts with the privacy interests of other individuals as well as the intellectual property rights of data controllers, and it also holds for the impact of data portability on competition and innovation.

14 Article 29 Working Party, "Guidelines on the right to data portability," 16/EN WP 242 rev.01, 5 April 2017, p. 11-12.

15 Article 29 Working Party, "Guidelines on the right to data portability," 16/EN WP 242 rev.01, April 5, 2017, p. 12.

16 For an analysis, see Inge Graef, Martin Husovec & Nadezhda Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law," German Law Journal 2018, p. 1375-1386.

17 Commission Communication, "A European strategy for data," COM(2020) 66 final, February 19, 2020, p. 13.

18 Facebook White Paper, "Charting a Way Forward on Privacy and Data Portability," September 2019, available at https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf.

19 Matthew Newman, "Facebook wants EU lawmakers to weigh up data portability's risks and rewards, Clegg says," MLex, December 2, 2019.

20 See the discussion in Inge Graef, "Paving the Way Forward for Data Governance: a Story of Checks and Balances (Editorial)," Technology and Regulation 2020, p. 26-27, available at https://techreg.org/index.php/techreg/article/view/57/13.

IV. POTENTIAL OF DATA PORTABILITY TO STIMULATE COMPETITION AND INNOVATION

It is still unclear what impact the GDPR's right to data portability exactly has on competition and innovation and if it can indeed foster competition between data controllers and encourage data-driven innovation, as was expected as a positive side effect of the new right at the time of adoption.[21] In particular, competition may increase in markets where data portability would make it easier for individuals to switch between services by taking their data with them.[22] A prerequisite for this is that individuals actively invoke their right to data portability.[23]

Despite its potential to stimulate competition and innovation, concerns are now expressed that data portability can strengthen the position of established players by letting their users invoke the right to data portability to get even more data.[24] This would lower competition because smaller firms would then see their users move with their data to the established players. For instance, economic modelling has suggested that data portability's prospect of easier switching can lure consumers into providing more data to the incumbent. Because of the additional data, the incumbent gets a competitive advantage in performing data analytics that can raise entry barriers for newcomers.[25] A recent review of economic literature expects data portability not to lead to less or more competition in established digital markets by itself, but does point at its ability to encourage innovation in complementary and new digital markets by letting innovation at the service and at the data analytics levels take place within different firms at the same time.[26]

V. ASYMMETRIC ENFORCEMENT OF THE GDPR'S RIGHT TO DATA PORTABILITY

A way to ensure that data portability creates opportunities for newcomers to innovate and that limits the undesirable effect of consolidating the market position of established players is to introduce asymmetric regulation and enforcement. Asymmetric enforcement implies that the level of obligations applicable to a business are tailored to its market share or the scope of its activities. In other words, powerful firms (which could for instance be determined by looking at whether they hold market power from the perspective of competition law) would be subject to stricter requirements for enabling data portability. The GDPR's risk-based approach already provides room for such an approach.

While the GDPR applies to all forms of processing of personal data regardless of the market position of the data controller, it does take into account the level of risk for determining the extent of the obligations to which controllers are subject. When the risk of processing is higher, data controllers have to comply with more detailed requirements. For instance, 'the risks of varying likelihood and severity for the rights and freedoms of natural persons' need to be taken into account for determining the extent of technical and organizational measures a data controller has to implement to ensure and be able to demonstrate that the processing of personal data is performed in compliance with the GDPR.[27] The 2019 expert report on 'Competition Policy for the Digital Era' commissioned by EU Commissioner Vestager also refers to the relevance of a firm's market power under the GDPR's risk-based approach.[28]

21 However, see the concerns about the costs that the GDPR's right to data portability would impose on small businesses expressed by Peter Swire & Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique," Maryland Law Review 2013, p. 349-353.

22 See the comments by the then Competition Commissioner Almunia in the speech "Competition and personal data protection," November 26, 2012, available at https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_860: 'I believe that a healthy competitive environment in these markets requires that consumers can easily and cheaply transfer the data they uploaded in a service onto another service. The portability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them'.

23 There are some indications that the GDPR's right to data portability is not so actively invoked or effectively implemented yet. See for instance Janis Wong & Tristan Henderson, "The right to data portability in practice: exploring the implications of the technologically neutral GDPR," International Data Privacy Law 2019, p. 173–191; Sarah Turner, July Galindo Quintero, Simon Turner, Jessica Lis & Leonie Maria Tanczer, "The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment," new media & society 2020 (forthcoming), p. 1-21, available at https://doi.org/10.1177/1461444820934033.

24 See also Esmeralda Florez Ramos & Knut Blind "Data portability effects on data-driven innovation of online platforms: Analyzing Spotify," Telecommunications Policy 2020, who argue that online platforms not facing real competition do not have a substantial need to increase investments in data-driven innovation due to possible risk and opportunity of increased user switching that could result from the GDPR's right to data portability.

25 Wing Man Wynne Lama & Xingyi Liu, "Does data portability facilitate entry?," International Journal of Industrial Organization 2020, p. 1-24, available at https://doi.org/10.1016/j.ijindorg.2019.102564.

26 Jan Krämer, Pierre Senellart & Alexandre de Streel, "Making data portability more effective for the digital economy: Economic implications and regulatory challenges," CERRE report June 2020, p. 55-64, available at https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/.

27 Article 24(1) GDPR.

28 Jacques Crémer, Yves-Alexandre de Montjoye & Heike Schweitzer, "Competition policy for the digital era," April 2019, p. 77, available at https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

In terms of compliance with Article 20 GDPR, asymmetric enforcement could mean that an additional responsibility is imposed on powerful data controllers to facilitate data portability. One of the open questions is whether the right to data portability requires one-off portability only, where personal data is transferred once to a new controller at the request of the data subject, or whether it can also be interpreted to include continuous and real-time portability of personal data until the data subject revokes her portability request. While some have argued that the GDPR's right to data portability has not been designed for real-time data sharing,[29] others have pleaded for a broader interpretation beyond one-off portability to make the right more suitable for the dynamic needs of data-driven markets.[30] Considering that data controllers with market power have more resources to implement the technical measures for enabling real-time portability, it would be justified to require such firms to do so in order to comply with Article 20 GDPR. This would make the GDPR's right to data portability more effective without burdening small data controllers with the same level of obligations. However, to avoid adverse effects on small data controllers, the compliance measures taken by powerful data controllers should be carefully monitored to prevent that technical standards are established that would squeeze out smaller firms or that would otherwise limit their ability to develop innovative services.

Criticism against making data protection obligations, such as the right to data portability, scalable may be that such an approach provides data subjects of data controllers holding market power with a higher level of protection as compared to data subjects of data controllers without market power. One could argue that this is at odds with the general applicability of the data protection rules. Furthermore, the fundamental right to data protection that the GDPR promotes requires to be respected irrespective of the market position of the data controller. After all, small data controllers may also engage in far-reaching data processing activities and can cause harm to their data subjects. However, there is reason to be particularly concerned about data controllers holding market power whose behavior is less constrained by the competitive forces of the market. In this regard, one could even claim that data subjects of powerful firms are less protected if the data protection rules would not take into account market power for interpreting the extent of protection to be offered to data subjects under the GDPR. Important to note here is that the scalability of data protection obligations would serve as a tool to impose stricter requirements on powerful data controllers and not to provide small businesses with an opportunity to bypass the minimum requirements laid down in the GDPR.[31]

VI. DATA PORTABILITY, COMPETITION ENFORCEMENT AND THE DIGITAL MARKETS ACT

Considering its hybrid nature, data portability is also relevant for competition enforcement. Market power is an inherent part of competition analysis, so that additional requirements can be imposed on powerful firms in several ways under competition law. Restrictions on data portability by dominant firms could be qualified as an exclusionary or exploitative abuse. Or a requirement to facilitate data portability could be imposed as a condition to approve a merger that gives rise to data-related competition concerns, for instance because the merging parties hold overlapping or complementary datasets. It is interesting to note in this regard that the European Commission has pointed at the right to data portability and other requirements in the GDPR as legal limits preventing competition concerns from arising in a number of merger cases.[32]

In its *Microsoft/LinkedIn* merger decision, the Commission argued that the applicability of data protection law limited Microsoft's ability to access and undertake any treatment of LinkedIn full data after the merger.[33] Although the merger was approved about 1.5 years before the GDPR started applying in May 2018, the Commission already pointed at the ability of the GDPR to 'further limit Microsoft's ability to have access and to process its users' personal data in the future' by strengthening the rights of data subjects such as through data portability.[34] As such, the Commission relied on (then still future) GDPR requirements to substantiate its reasoning that the combination of datasets of the two merging parties did not raise competition concerns. Even more remarkably, in its *Google/Sanofi* merger decision the Commission relied on the ability of the GDPR's right to data portability to prevent diabetes patients from becoming locked-in to a digital e-medicine platform to be offered by the future joint venture while the text of the GDPR was not even adopted at the time the merger was approved.[35]

29 Jacques Crémer, Yves-Alexandre de Montjoye & Heike Schweitzer, "Competition policy for the digital era," April 2019, p. 81-82.

30 Josef Drexl, "Data access and control in the era of connected devices: Study on Behalf of the European Consumer Organisation BEUC," 2018, p. 110, available at https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf.

31 For a detailed discussion, see Inge Graef & Sean van Berlo, "Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come With Greater Responsibility," European Journal of Risk Regulation (forthcoming).

32 For a detailed discussion, see Inge Graef, Damian Clifford & Peggy Valcke, "Fairness and enforcement: bridging competition, data protection, and consumer law," International Data Privacy Law 2018, p. 215-217.

33 Case M.8124 - Microsoft/LinkedIn, December 6, 2016, par. 254–255 and 375.

34 Case M.8124 - Microsoft/LinkedIn, December 6, 2016, par. 178.

35 Case M.7813 - Sanofi/Google/DMI JV, 23 February 2016, par. 67-69. Note that the final text of the GDPR was adopted on April 27, 2016.

Although the integration of GDPR requirements into merger analysis is a welcome development for the coherent application of different regimes of EU law, it also gives rise to risks when the conclusion that competition concerns are absent assumes compliance with and effective enforcement of existing, and let alone future, data protection rules. As acknowledged by the Commission in its June 2020 Communication evaluating the two years of application of the GDPR, a bottleneck in current data protection enforcement against big tech firms is that they are typically established in Ireland and Luxembourg. Because the GDPR automatically assigns the national data protection authority of the data controller's main establishment as the lead supervisory authority for the entire EU, the Irish and Luxembourg data protection authorities have to act as lead authorities in many important cross-border cases for which they need larger resources than their population would otherwise suggest.[36]

Considering these enforcement problems in data protection law, the Commission could make compliance with the GDPR (or at least those GDPR requirements relevant to the merger analysis) a condition for approving a data-driven merger to prevent that competition concerns occur afterwards because data protection rules like the GDPR's right to data portability are not effectively implemented or enforced. This would give the Commission the ability to intervene itself if necessary after the merger when competition concerns still occur because of a lack of data protection compliance by the merged entity and a lack of enforcement by data protection authorities. Even though the GDPR is now in full force, its ability to prevent competition concerns from arising due to the limits it imposes on merging parties to combine their datasets is still suffering from the enforcement issues.

Beyond competition enforcement, the European Commission is currently preparing a legislative proposal to adopt a Digital Markets Act. The Digital Markets Act will include ex ante regulation for so-called gatekeeping platforms.[37] Data portability could be one of the ex ante obligations imposed on these platforms. While there are still questions about how to design and enforce requirements of data portability under competition law and new ex ante regulation, their asymmetric approach would be welcome in an effort to increase the opportunities for smaller firms and newcomers to compete and make markets more contestable.

In particular, competition enforcement and new ex ante regulation are not bound by the limits set by the GDPR's right to data portability. Data portability is also relevant in business-to-business relations where business users may face difficulties in switching service providers when they cannot take their business data with them.[38] To make data portability effective for dynamic digital markets (such as the Internet of Things),[39] real-time and continuous data portability would be required. This could be implemented through requirements on dominant firms or gatekeeping platforms (either within or beyond the GDPR as discussed in section V. above). Furthermore, the scope of application of the GDPR's right to data portability is limited to personal data 'provided by' the data subject. This notion is interpreted by the Article 29 Working Party as including data knowingly and actively provided by the data subject (such as one's contact details or age) as well as data observed by virtue of the data subject's use of a service or device (such as one's search history). However, inferred or derived data created by the data controller through subsequent analysis of provided or observed data (such as algorithmic results or results of user profiling) are excluded from the scope.[40] Since inferred or derived data carry a lot of value and would be particularly relevant for enabling competition in markets for data analytics, data portability requirements enforced against dominant or gatekeeping platforms through competition law and new ex ante regulation could include such data.

36 Commission Communication, "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation," COM(2020) 264 final, June 24, 2020, p. 5-6.

37 European Commission, "Inception Impact Assessment of the Digital Services Act Package," Ares(2020)2877686 , July 2, 2020, available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services.

38 See the self-regulatory codes of conduct that the Commission should facilitate to enable businesses to port data and switch cloud service providers based on Article 6 of Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59.

39 See also Jan Krämer, Pierre Senellart & Alexandre de Streel, "Making data portability more effective for the digital economy: Economic implications and regulatory challenges," CERRE report June 2020, p. 79-83.

40 Article 29 Working Party, "Guidelines on the right to data portability," 16/EN WP 242 rev.01, 5 April 2017, p. 9-11.

VII. BEYOND DATA PORTABILITY

Despite its potential to empower individuals or business users in their individual relationship with a data controller, a question is whether data portability (irrespective of whether it is enforced under the GDPR, competition law, or new ex ante regulation and irrespective of how expansive its scope is interpreted) is enough to stimulate competition and innovation in data-driven markets. How data portability affects competition and innovation will mainly depend on how actively individuals and businesses overall request transfers of their data. In order for overall competition in data-driven markets to increase, it is not enough that just a few individuals or businesses invoke data portability.

To address risks of market tipping and increasing market concentration in data-driven industries, requirements for market players to share data directly with competitors or new entrants may be needed in certain circumstances.[41] This would mean that the exchange of data is no longer dependent on a portability request of an individual or a business. Data protection and privacy interests of course have to be taken into account when personal data is involved. Illustrative here is that the UK Competition and Markets Authority ("CMA") recommended in its July 2020 market study into online platforms and digital advertising to require Google to open up its click and query data to allow rival search engines to properly compete by improving their algorithms. According to the UK CMA, such an intervention can be designed in a way that does not involve the transfer of personal data to prevent data protection concerns.[42]

Porting of data creates a positive externality through the better service (in terms of better predictions or search results for instance) that all users will receive when an additional user brings her data to a new provider. However, users typically do not take this benefit for other users into account when deciding to port data, so that we should expect too little data portability requests to remedy market tipping.[43] To stimulate data-driven innovation, there is a need to consider additional data access requirements beyond data portability.[44]

VIII. CONCLUSION

Data portability has a hybrid nature. What emerged as a data protection concept is now also becoming part of policies aiming to stimulate competition and innovation. To reap the full benefits of data portability, this article has argued that there is a need for regulators to steer its implementation and to provide guidance on how data controllers should handle tensions between different interests and overlapping legal entitlements. Data portability can empower individuals and business users to make better choices but more asymmetric enforcement is needed to ensure that data portability will stimulate competition.

Merger analysis should not assume effective enforcement of GDPR requirements, like the right to data portability, if they are determinative for the question whether a data-driven merger raises competition concerns. Instead, competition authorities should proactively consider the imposition of conditions for approving a data-driven merger to prevent that competition concerns occur afterwards because data protection rules are not complied with. And as a tool to promote data-driven innovation, data portability is a necessary but probably not a sufficient condition to keep markets open to newcomers.

41 Cédric Argenton & Jens Prüfer, "Search Engine Competition with Network Externalities," Journal of Competition Law and Economics 2012, p. 73-105 and Jens Prüfer & Christophe Schottmüller, "Competing with Big Data," Journal of Industrial Economics (forthcoming), available as TILEC Discussion Paper No. 2017-006 at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918726.

42 UK CMA, "Online platforms and digital advertising Market study final report," July 1, 2020, p. 365-367, available at https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf.

43 Inge Graef & Jens Prüfer, "Mandated data sharing is a necessity in specific sectors," Economisch Statistische Berichten 2018, p. 300, available at https://esb.nu/incoming/20042404/mandated-data-sharing-is-a-necessity-in-specific-sectors.

44 For a discussion, see Bertin Martens, Alexandre de Streel, Inge Graef, Thomas Tombal & Néstor Duch-Brown, "Business-to-Business data sharing: An economic and legal analysis," *JRC Digital Economy Working Paper 2020-05* July 2020, available at https://ec.europa.eu/jrc/sites/jrcsh/files/jrc121336.pdf; and Richard Feasey & Alexandre de Streel, "Data Sharing for Digital Markets Contestability: Towards a Governance Framework," CERRE report September 2020, available at https://cerre.eu/publications/data-sharing-digital-markets-competition-governance/.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.